REMARKS

Claims 1-14 are pending in this application. Claims 1, 3, 7 and 9 have been amended by way of the present amendment. Reconsideration is respectfully requested.

In the outstanding Office Action claim 3 was objected to because an informality of lack of clarification; claim 7 was objected to because of an informality of a missing word; claims 7 and 9 were rejected under 35 USC § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention; claims 1-14 were rejected under 35 USC § 102(b) as being anticipated by U.S. Patent No. 6,233,565 (Lewis et al.).

Claim Objections

Claim 3 was objected to because an informality of lack of clarification; claim 7 was objected to because of an informality of a missing word. Reconsideration is respectfully requested.

Claim 3 has been amended to clarify the invention and in particular, that clarify a function of the "slave cryptographic unit *to retrieve requested information*" (emphasis added) In particular, as shown below claim 3 has been amended as follows:

> responding to the key confirmation message with a downloading message to allow the slave cryptographic unit ~~retrieving~~ to retrieve requested information; and
>
> sending a finish message to the master cryptographic unit after the requested information is completely downloaded.

In addition, claim 7 has been amended to correct the informality of a missing word. Specifically, claim 7 has been amended to recite:

> further comprising a step of sending the ~~rest~~ reset message to request the master cryptographic unit to validate an initial key held by the slave cryptographic unit.

Support for the amendments is provided at least at paragraph **[0007]**, lines 10-13, and lines 2-7, respectively, of the filed specification. Therefore, it is respectfully submitted that the amended claims raise no question of new matter and clarify the invention. Therefore, it is respectfully requested that the outstanding objections be withdrawn.

35 USC § 112 Claim Rejections

Claims 7 and 9 were rejected under 35 USC § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

Claims 7 and 9 have been amended to further clarify the invention. As discussed above, claim 7 has been amended to replace the term "rest" with "reset." Claim 9 has been similarly amended. Therefore, it is respectfully submitted that "the reset message" has proper antecedent basis and it is requested that the outstanding rejections are now moot and should be withdrawn.

35 USC § 102 Claim Rejections

Claims 1-14 were rejected under 35 USC § 102(b) as being anticipated by Lewis et al. Reconsideration is respectfully requested.

First, it is respectfully submitted that anticipation requires the disclosure, in a prior art reference, of *each and every limitation* as set forth in the claims (emphasis added).[1] There must be no difference between the claimed invention and reference disclosure for an anticipation rejection under 35 U.S.C. §102.[2] To properly anticipate a claim, the reference *must teach every element of the claim* (emphasis added).[3] "A claim is *anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described*, in a single prior art reference (emphasis added)."[4] "The identical invention must be shown in as complete detail as is contained in the ... claim."[5] In determining anticipation, *no claim limitation may be ignored* (emphasis added).[6]

Claim 1 has been amended to clarify the invention. In particular, claim 1 has been amended to recite:

> sending either a reset message or a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit during each session.

Support for the amendment is provided at least at paragraph **[0005]**, lines 2-3 of the filed specification. Therefore, it is respectfully submitted that the amendment raises no question of new matter.

Lewis et al. discloses a system and methods for conducting Internet based financial transactions between a client and a server.[1] In particular, Lewis et al. discloses a HouseKeeping Service that queries the server **4** to ensure that current keys have not expired and that, if the keys are about to expire, the client **2n** will issue a command to renew the keys and a new public key

[1] Lewis et al. at ABSTRACT.

will be sent back to the server **4**.[2] Further, Lewis et al. discloses a Crypto Officer State **940** is entered only when the key file needs to be updated and that this will happen either when the user changes the password or when the current RSA keys expire and need to be changed.[3] Moreover, Lewis et al. discloses that the server **4,** during authentication, will trigger replacement of expired keys.[4]

However, Lewis et al. nowhere discloses, as amended claim 1 recites:

> sending either a *reset message or a key validation message* to request the master cryptographic unit to validate a key held by the slave cryptographic unit *during each session* (emphasis added).

That is, as discussed above, Lewis et al. discloses the client **2** renewing keys, updating keys when the user changes the password or when the current RSA keys expire. However, does not disclose the key file needs to be renewed, updated or that the current RSA key needs to be replaced by a new RSA key "during each session," as recited in amended claim 1. Moreover, in contrast to the claimed invention, Lewis et al. nowhere discloses sending "either a reset message or a key validation message to request the master cryptographic unit to *validate a key held by the slave cryptographic unit during each session"* (emphasis added).

Further, the applied art does not disclose a method of secure data exchange between a master cryptographic unit and a slave cryptographic unit, wherein the method includes, among other features, "sending either a reset message or a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit during each session; and forwarding a key exchange message, which includes a new key encrypted through the key held by the slave cryptographic unit, from the master cryptographic unit to the slave cryptographic unit", as recited in independent claim 1, as amended.

Furthermore, the present claimed invention is based on the exchange of cryptographic keys between two cryptographic units and a new key replaces a previous key during each session

[2] *Id.* at column 23, lines 53-57.
[3] *Id.* at column 24, lines 44-47.
[4] *Id.* at column 24, lines 46-48.

so that an eavesdropper steals too little cyphertext to complete cryptanalysis during an insufficient period of each session. In contrast to Applicants' disclosed and claimed invention, in Lewis et al., the key file needs to be updated when some specific occasions happen, and the current RSA keys need to be changed when they expire. Thus, in Lewis et al. it appears that an eavesdropper can steal sufficient cyphertext to complete cryptanalysis during a long period of several sessions or numerous sessions.

Conclusion

In view of the above amendments and remarks, Applicants believe that each of pending claims 1-14 in this application is in immediate condition for allowance. An early indication of the same would be appreciated.

Conclusion

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necesssary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22171-00018-US1 from which the undersigned is authorized to draw.

Dated: July 2, 2007

Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111 (Tel)
(202) 293-6229 (Fax)
Agent for Applicant